Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung 27.10.2008
Unterarbeitsgruppe EU-Dienstleistungsrichtlinie/IMI

Datenschutzrechtliche Grundanforderungen
bei der Umsetzung der EU-Dienstleistungsrichtlinie

(von der 76. DSK in Bonn am 6./7. November 2008 zustimmend zur Kenntnis genommen)

Die EU-Dienstleistungsrichtlinie regelt die freie grenzüberschreitende Erbringung von Dienstleistungen in einem europäischen Binnenmarkt und dies bei gleichen Bedingungen für die Geschäftstätigkeit aller Dienstleister. Eine am Abbau von bürokratischen Hindernissen und an mutmaßlichen Bedürfnissen von Dienstleistern orientierte integrierte Verwaltungsorganisation soll mittels *einheitlicher* (behördlicher) *Ansprechpartner* und neuer elektronischer Kommunikationsinfrastrukturen online über das Internet sichergestellt werden, Art. 6 und 7, 8 Abs. 1 *RL 206 /123/EG*. Vorgesehen ist in der Bundesrepublik Deutschland, behördliche Wege und Infrastruktur nicht nur für grenzüberschreitende Vorgänge sondern auch für die inländischen Abläufe einzurichten.

1. Zielkonflikt mit datenschutzfreundlichen Grundsätzen

Personenbezogene Datenverarbeitung hat zweckgebunden zu erfolgen. Die zu schaffenden gesetzlichen Vorschriften zur Umsetzung der Richtlinie haben den Zweck der personenbezogenen Datenverarbeitung genau festzulegen und zu beschränken. Das Zweckbindungsgebot führt letztendlich dazu, dass ein Datenaustausch zwischen Behörden nicht ohne weiteres zulässig ist (Grundsatz der informationellen Gewaltenteilung). Sollen aber schon Datenflüsse gebündelt oder konzentriert werden, wie es die Richtlinie vorsieht, so sind gleichwohl dem Trennungsgebot folgend, informationelle Datenverbünde weitestgehend zu minimieren und zu vermeiden. Dies ist gesetzlich und mit Verfahrensvorschriften sicherzustellen.

2. Pflicht zur Aufgabenzuweisung mittels gesetzlicher Vorschriften

Das Handeln öffentlicher Stellen, die die Verarbeitung personenbezogener Daten durchführen, hat auf der Grundlage gesetzlicher Vorschriften zu erfolgen, BVerfGE 65, 1ff. Dem *Einheitlichen Ansprechpartner* werden nach der Richtlinie eigene umrissene Aufgaben und Zuständigkeiten übertragen, vgl. Art. 7 Abs. 4, 11 Abs. 3 *RL 206 /123/EG*. Datenschutzrechtlich ist der *Einheitliche Ansprechpartner* damit nicht Auftragnehmer (einer Datenverarbeitung im Auftrag), sondern eigene *datenverarbeitende* und *verantwortliche Stelle*. Im Zweifel wäre eine entsprechende Klarstellung durch den Gesetzgeber vorzunehmen.

Verfassungsrechtlich sind also bei der Umsetzung der Richtlinie eine normenklare gesetzliche Grundlage der Datenverarbeitung und eine präzise Aufgabenzuweisung erforderlich, die es dem Einzelnen möglich machen, Inhalt, Umfang und Ausmaß der Datenverarbeitung bestmöglich abzuschätzen. Insbesondere ist dabei klarzustellen, in welcher Tiefe durch den *Einheitlichen*

Ansprechpartner Daten in Abgrenzung zu den letztendlich entscheidenden Stellen verarbeitet werden sollen. Anzuraten ist bereits eine konkrete Regelung in einem formellen Gesetz, erforderlich ist mindestens eine Verordnungsermächtigung im formellen Gesetz zur Regelung weiterer Einzelheiten per Rechtsverordnung.

3. Spezielle und bereichsspezifische *Datenverarbeitungsregeln*

Die sich in Teilen überlagernde Zuständigkeit der für ein Verfahren *zuständigen Behörde* und der des *Einheitlichen Ansprechpartners* als überwachende, kontrollierende, verfahrensbegleitende oder Verfahrens- und Dokumentationspflichten wahrnehmende Stelle führt unweigerlich zu der Fragestellung, welche personenbezogenen Daten der *Einheitliche Ansprechpartner* überhaupt erheben, speichern, übermitteln, im Detail zur Kenntnis nehmen soll und wann er die bei ihm gespeicherten Daten löschen. muss. Seine Aufgaben sind von denen der jeweils fachlich zuständigen Stellen abzugrenzen. Die EU-Dienstleistungsrichtlinie weist ausdrücklich darauf hin, dass mit der Einrichtung des Einheitlichen Ansprechpartners nicht in bestehende Zuständigkeiten eingegriffen werden soll (Art. 6 Abs. 2 *RL 206 /123/EG*). Letztendlich bleibt der Inhalt des Vorgangs mit der damit einhergehenden Datenverarbeitung bei der jeweils *zuständigen Behörde*. Da dem *Einheitlichen Ansprechpartner* mehr koordinierende und überwachende Funktionen zukommen, darf durch ihn im Sinne der Erforderlichkeit nicht die gleiche Datenverarbeitung wie durch die *zuständigen Behörden* selbst erfolgen. Eine dem Gesetzesvorbehalt genügende Gesetzgebung erfordert daher die Schaffung spezieller bzw. bereichspezifischer Gesetzesregelungen zur Datenverarbeitung für den *Einheitlichen Ansprechpartner*. Diese Regelungen müssen, um doppelte Datenverarbeitung zu vermeiden oder wenigstens zu minimieren, die Verarbeitung personenbezogener Daten durch den *Einheitlichen Ansprechpartner* auf das zur Aufgabenerfüllung erforderliche Maß beschränken. Es sind normenklare Datenverarbeitungsbefugnisse und -regeln festzulegen:

- für die Erhebung der für die Aufgabenerfüllung des ‚*Einheitlichen Ansprechpartners* unbedingt erforderlichen Daten
- zur Erforderlichkeit der Kenntnisnahme von Einzeldaten und für die Speicherung von Daten,
- für Datenübermittlungen zwischen EAP und den *zuständigen Behörden*,
- zur Zweckbindung (einschließlich des grundsätzlichen Verbots personenbezogene Daten aus verschiedenen Verfahren abzugleichen),
- zur Verarbeitung sensibler Daten,
- für die Löschung und Archivierung (einschließlich Fristen, Zuständigkeiten).

Zusätzliche bereichsspezifische Normierungen der Datenverarbeitung des *Einheitlichen Ansprechpartners* gegenüber einem allgemeinen Gesetz können zudem zu einem datenschutzgerechteren Umgang und zu mehr Rechtssicherheit bei *zuständigen Behörden* und *Einheitlichen Ansprechpartnern* führen.

4. Betroffenenrechte

Wesentlicher Baustein einer datenschutzgerechten Normgebung und Umsetzung sind normenklare Regelungen der Betroffenenrechte, die dem Einzelnen auch gegenüber dem *Einheitlichen Ansprechpartner* zustehen müssen.

Geregelt sein sollte darüber hinaus auch, ob Anträge auf

- Löschung,
- Berichtigung,
- Auskunft und Akteneinsicht und
- Widerspruch gegen die Datenverarbeitung

(auch) an den *Einheitlichen Ansprechpartner* gerichtet werden können sollen, wenn sie sich auf die personenbezogene Datenverarbeitung der *zuständigen Behörde* beziehen. Benachrichtigungspflichten an die Betroffenen, z. B. bei der Weiterleitung von Unterlagen (Daten), sollten zudem geregelt werden.

Aufgrund der möglichen Überlagerungen der Datenverarbeitung empfiehlt sich eine Annahme der Betroffenenanträge sowohl beim *Einheitlichen Ansprechpartner*, als auch bei den *zuständigen Behörden*, die dann zumindest die Anträge an die jeweils *datenverarbeitende Stelle* weiterzuleiten haben.

5. Datenschutzfreundliche Umsetzung

Die in den Datenschutzgesetzen bestimmten Grundsätze der *Datensparsamkeit* und *Datenvermeidung* sind bereits bei der Normsetzung in Bezug auf die Folgen, letztendlich aber auch beim Gesetzesvollzug zu beachten. Hierbei hat man sich an den nach der *RL 206 /123/EG* festgelegten Pflichtaufgaben zu orientieren. Von der Übertragung von über die *RL 206 /123/EG* hinausgehenden Aufgaben ist schon zur Vermeidung von Doppelzuständigkeiten abzusehen. Verfahrensrechtlich benötigt der *Einheitliche Ansprechpartner* nur die aufgabenbedingten Antragsdaten (regelmäßig aber nicht komplette Anträge mit weitergehenden Angaben), was bei der Normsetzung bereits zum Ausdruck gekommen sein sollte. Den beschränkten Aufgaben des *Einheitlichen Ansprechpartners* hat die Datenverarbeitung im Hinblick auf Umfang, Tiefe und Ausmaß zu folgen. Dabei müssen auch in der technischen Umsetzung Ansätze zur Datensparsamkeit verfolgt werden. In diesem Zusammenhang sei auf die Überlegungen eines technischen Ansatzes hingewiesen, mit dem der Antragsteller mit Hilfe des *Einheitlichen Ansprechpartners* zur Direktkommunikation mit der *zuständigen Behörde* geleitet wird, der auch für die Verwaltung effizienter und weniger belastend ist (vgl. z. B. Rost, VM (Zeitschrift für Verwaltung und Management) 2008, S. 220 ff.). Aus Datenschutzsicht ist solchen Lösungsmodellen, die die Anreicherung von Daten beim *Einheitlichen Ansprechpartner* vermeiden helfen, der Vorzug zu geben.

6. Umsetzung von Datensicherheitsanforderungen

In Bezug auf die technische Umsetzung der *RL 206 /123/EG* gilt nichts anderes als für andere automatisierte Verfahren und Infrastrukturen auch. Es ist ein *Datenschutz- und Datensicherheitskonzept* zu erstellen, gesetzlich erforderliche *Vorabkontrollen* sind durchzuführen. Auf das technische Verfahren haben *Risikomanagement- und Qualitätsmanagementmechanismen* zur Anwendung zu kommen.

Insbesondere sind bei vorgesehener elektronischer Kommunikation

- eine sichere Authentifizierung (siehe Entschließung der DSB-Konferenz „Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren“ vom 11. Oktober 2006),
- elektronische Nachweisverfahren (z. B. bei der Einreichung von Belegen und Urkunden) und
- eine dauerhafte gerichtsfeste Erhaltung von Dokumenten und elektronischen Entscheidungen

sicherzustellen.

Nicht abschließend geklärt sind und einer Lösung zugeführt werden müssen insbesondere die Fragen der gesicherten Übermittlung und Langzeitarchivierung digital signierter Dokumente aus dem EU-Ausland.

Soweit verschiedene Vorhaben und Verfahren, Verfahren zum *Einheitlichen Ansprechpartner*, IMI, D115 umgesetzt werden sollen, die sich z. T. überschneiden, sind diese bereits frühzeitig aufeinander abzustimmen oder besser voneinander abzugrenzen.

Weitere datenschutzrechtliche und sicherheitstechnische Hinweise sind dem Arbeitspapier *Der „Einheitliche Ansprechpartner“ nach der Dienstleistungsrichtlinie – Aspekte des Datenschutzes und der Datensicherheit“* zu entnehmen (Anlage B8 zum Projektbericht „Deutschland-Online-Vorhaben IT-Umsetzung der Europäischen Dienstleistungsrichtlinie“, herunter ladbar unter http://213.216.17.150/DOL/Anlagen/Anlage_B8_Beitrag_Datenschutz.pdf).